Version 1.0

IT DATA PROTECTION AND INFORMATION SECURITY POLICY

ECOS (I) Mobility & Hospitality Ltd.

INFORMATION ON THE DOCUMENT

Type of Document	**Policy**
Main Policy Statement	Eco Mobility is committed to ensuring the secure, responsible, and efficient use of information and technology resources to support business operations, protect stakeholder information, maintain regulatory compliance, and strengthen business resilience.
Document Valid from	28th May, 2026
Minimum Period of revision	1 year
Version	1.0
Version effective from	28th May, 2026
Created by	HR Head
Reviewed by	Chief Operating Officer
Approved by	Board of Directors

1. POLICY STATEMENT

Eco Mobility recognizes that information, technology, and digital infrastructure are critical enablers of business operations, customer experience, regulatory compliance, and sustainable growth. The Company is committed to maintaining a secure, resilient, and responsible digital environment that protects information assets, supports business continuity, promotes stakeholder trust, and aligns with the Company's Environmental, Social and Governance (ESG) commitments.

The Company acknowledges that cybersecurity, information security, data privacy, and responsible technology governance are integral components of enterprise risk management and corporate governance. Accordingly, the Company shall establish and maintain appropriate governance structures, controls, processes, and awareness mechanisms to protect information assets against unauthorized access, misuse, disclosure, alteration, destruction, or disruption.

This Policy reflects the Company's commitment to safeguarding customer, employee, shareholder, vendor, and business information while ensuring compliance with applicable laws and regulations.

2. PURPOSE

The purpose of this Policy is to establish a governance framework for the secure and responsible management of information and technology resources across the Company.

The Policy aims to:

- Protect the confidentiality, integrity, and availability of information assets.
- Promote responsible and ethical use of technology.
- Strengthen cybersecurity and operational resilience.
- Safeguard personal and business information.
- Support compliance with applicable legal and regulatory requirements.
- Enhance stakeholder trust and confidence.
- Integrate digital responsibility within the Company's ESG framework.
- Promote continuous improvement in information security and cyber resilience.

3. SCOPE AND APPLICABILITY

This Policy applies to all directors, officers, employees, consultants, contractual personnel, temporary staff, service providers, vendors, business partners, and any other persons who access, process, store, transmit, or manage information on behalf of the Company.

The Policy applies to all information assets irrespective of format, including electronic records, cloud-based information, databases, applications, communication systems, mobile devices, physical records, and other technology resources owned, leased, operated, or managed by the Company.

Compliance with this Policy is mandatory.

4. ESG COMMITMENT TO DIGITAL RESPONSIBILITY

The Company recognizes that responsible management of information and technology contributes directly to sustainable business practices and long-term value creation.

From a Governance perspective, the Company is committed to maintaining robust cybersecurity, privacy, risk management, and information governance practices supported by Board oversight and management accountability.

From a Social perspective, the Company recognizes its responsibility to protect personal information entrusted by customers, employees, vendors, investors, and other stakeholders and to use technology in a fair, transparent, and responsible manner.

From an Environmental perspective, the Company encourages efficient use of digital resources, reduction of paper-based processes, responsible lifecycle management of technology assets, and environmentally responsible disposal of electronic equipment and storage media.

The Company shall continually strengthen its digital resilience and information security posture to support stakeholder trust and sustainable growth.

5. GOVERNANCE AND ACCOUNTABILITY

The Board of Directors shall provide oversight of information security, cybersecurity, digital risk management, and data protection matters as part of the Company's governance framework.

The Audit Committee and Risk Management Committee, where applicable, shall periodically review material technology risks, cybersecurity incidents, compliance matters, and mitigation measures.

Senior Management shall ensure adequate resources, systems, and processes are established to implement this Policy effectively.

The Information Technology function shall be responsible for implementing appropriate security controls, monitoring risks, managing technology resources, and responding to incidents.

The designated Grievance Officer and such other officers as may be required under applicable law shall oversee privacy related complaints, regulatory coordination, and data protection matters.

Every employee, contractor, and user of Company information systems shall share responsibility for protecting Company information and complying with this Policy.

6. INFORMATION SECURITY PRINCIPLES

The Company shall implement appropriate administrative, technical, and physical safeguards to protect information assets throughout their lifecycle.

Information shall be protected against unauthorized access, disclosure, alteration, loss, theft, misuse, destruction, or disruption.

Security measures shall be proportionate to the nature of the information being processed, applicable legal requirements, business needs, and identified risks.

The Company shall adopt a risk based approach to information security and continuously review emerging threats, vulnerabilities, and control effectiveness.

7. DATA PRIVACY AND DATA PROTECTION

The Company is committed to processing personal data lawfully, fairly, transparently, and responsibly as per Digital Personal Data Protection Act, 2023 and Company's Policy on Digital Personal Data Protection.

Personal data shall be collected only for legitimate business purposes and shall be retained ,as per Retention Schedule, and only for as long as necessary to fulfil those purposes or meet legal and regulatory obligations.

Appropriate safeguards shall be implemented to protect personal data against unauthorized access, misuse, disclosure, loss, or destruction.

The Company shall establish processes for handling privacy related requests, grievances, complaints, and incidents in accordance with applicable law.

Appropriate contractual safeguards shall be maintained where personal data is processed by third parties on behalf of the Company.

The Company shall take reasonable measures to protect customer travel, location, booking, and transportation-related information from unauthorized access, disclosure, or misuse.

8. ACCESS MANAGEMENT

Access to Company information systems and information assets shall be granted based on business need, job responsibilities, and the principle of least privilege.

User access shall be appropriately authorized, periodically reviewed, modified when roles change, and revoked promptly upon separation from the Company.

The Company may implement authentication, authorization, monitoring, and access control measures necessary to protect information assets and systems.

9. CYBERSECURITY AND TECHNOLOGY CONTROLS

The Company shall maintain appropriate cybersecurity measures to identify, prevent, detect, respond to, and recover from cyber threats and security incidents.

Such measures may include endpoint protection, network security controls, vulnerability management, system monitoring, encryption, backup arrangements, and other security controls as determined appropriate by Management.

Technology standards and operating procedures may be prescribed separately by the Information Technology function and updated periodically to address evolving risks and business requirements.

10. THIRD-PARTY RISK MANAGEMENT

The Company recognizes that third party relationships may introduce information security and privacy risks.

Appropriate due diligence shall be conducted before engaging third parties that have access to Company information, systems, or personal data.

Contracts with such third parties shall include appropriate confidentiality, information security, privacy, incident reporting, and compliance obligations.

Third-party risks shall be monitored throughout the engagement lifecycle.

11. INCIDENT MANAGEMENT AND CYBER RESILIENCE

The Company shall establish procedures for identifying, reporting, investigating, managing, and responding to information security incidents and cybersecurity events.

All personnel are expected to promptly report actual or suspected security incidents, privacy concerns, vulnerabilities, or policy violations.

Material incidents shall be escalated through appropriate management and governance channels.

The Company shall seek to learn from incidents and continuously strengthen its security posture through corrective and preventive measures.

12. BUSINESS CONTINUITY AND OPERATIONAL RESILIENCE

The Company shall maintain appropriate business continuity and disaster recovery arrangements to support critical business operations during disruptions.

Business continuity planning shall consider technology failures, cyber incidents, data loss, natural disasters, operational disruptions, and other significant risks.

Periodic testing and review of continuity arrangements shall be conducted to assess preparedness and resilience.

13. TRAINING AND AWARENESS

The Company shall promote a culture of cybersecurity awareness and responsible information handling.

Employees and relevant stakeholders shall receive periodic training and awareness programs covering information security, data protection, cyber threats, privacy obligations, and responsible use of technology.

Management shall encourage continuous learning and awareness to address evolving technology and security risks.

14. MONITORING, REVIEW AND CONTINUOUS IMPROVEMENT

The Company may periodically monitor and review key information security and privacy indicators, including employee awareness training coverage, cybersecurity incidents, data privacy complaints, and remediation effectiveness.

Internal reviews, risk assessments, audits, and management evaluations may be conducted to identify opportunities for improvement.

The Company shall continually enhance its information security framework in response to evolving business requirements, regulatory developments, technological changes, and emerging threats.

15. POLICY VIOLATIONS

Failure to comply with this Policy may result in disciplinary action, restriction of access privileges, contractual remedies, recovery of losses, or legal action, as appropriate and in accordance with applicable laws and Company policies.

The Company encourages prompt reporting of genuine concerns and shall not tolerate retaliation against individuals reporting concerns in good faith.

16. REPORTING CONCERNS

Employees and third parties are encouraged to report any suspected violations of this policy promptly. Reports may be made to:

It is the duty of all those covered under this policy to comply with this policy and report any concern or information that they may have in relation to the violation of this provision of this document in respect of breach of Information Security. The report may be submitted to HR email id: hr@ecosmobility.com or at peoplehotline@ecosmobility.com. In case concern has to be raised to compliance officer, you may reach out to legal@ecosmobility.com.

(b) Alternatively, concerns on the violations of the company policies may be reported through the Whistle Blower mechanism viz whistleblower@ecosmobility.com or in exceptional matters at erwbc@ecosmobility.com. A person reporting may choose to remain anonymous.

17. POLICY REVIEW

This Policy shall be reviewed annually or earlier if required due to changes in business operations, technology, regulatory requirements, emerging risks, or significant incidents.

Any material amendments shall be placed before the Board of Directors or the appropriate authority for approval.

Frequently Asked Questions (FAQ)

1. Who is required to comply with this Policy?

Answer:
All directors, employees, interns, consultants, contractual staff, vendors, service providers, and any person accessing Company information or systems must comply with this Policy.

2. What should I do if I receive a suspicious email or message?

Answer:
Do not click on links, download attachments, or respond to the sender. Immediately report the email to the IT Team or the designated reporting channel.

3. What is considered a cybersecurity incident?

Answer:
Examples include:

- Phishing emails
- Malware or ransomware attacks
- Unauthorized access to systems
- Loss or theft of Company devices
- Data leaks or accidental disclosure of information
- Password compromise

4. What is personal data?

Answer:
Personal data refers to any information relating to an identifiable individual, such as name, phone number, email address, employee records, customer information, identification numbers, or location data.

5. What should I do if I accidentally send confidential information to the wrong person?

Answer:
Immediately report the incident to the IT Team, HR, or Compliance Team. Prompt reporting enables the Company to take corrective actions and minimize risk.

6. What should vendors or third parties do if they identify a security issue?

Answer:
Vendors and third parties must promptly notify the Company through the designated contact channels and cooperate in addressing the issue.

7. What happens if someone violates this Policy?

Answer:

Violations may result in disciplinary action, restriction of system access, contractual remedies, recovery of losses, or legal action, depending on the nature and severity of the violation.